115

JAMES R. BUSSELLE (SBN 75980)
THOMAS E. MOORE III (SBN 115107)
MARY O'BYRNE, (SBN 121067)
TOMLINSON, ZISKO, MOROSOLI & MASER
200 Page Mill Road, Second Floor
Palo Alto, California 94306
Telephone: (415) 325-8666

Attorneys for Defendant
RSA Data Security, Inc.

TOMLINSON, ZISKO, MOROSOLI & MASER
ATTORNEYS AT LAW
200 PAGE MILL ROAD, SECOND FLOOR
PALO ALTO, CALIFORNIA 94306
(415) 325-8666

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

ROGER SCHLAFLY, Plaintiff, vs. PUBLIC KEY PARTNERS and RSA DATA SECURITY, INC., Defendants.	CASE NO.: C 94 20512 SW (PVT) DECLARATION OF CLAUS P. SCHNORR IN OPPOSITION TO PLAINTIFF'S MOTION FOR PARTIAL SUMMARY JUDGMENT DATE: December 6, 1995 TIME: 10:00 a.m. BEFORE: Hon. Spencer Williams

I, Claus P. Schnorr, declare:

1. I am one of the inventors of U.S. Patent No. 4,995,082, "Method for identifying Subscribers and for Generating and Verifying Electronic Signatures in a Data Exchange System." I have personal knowledge of each and every fact set forth below and can competently testify thereto.

2. I applied for a U.S. patent on my invention on or about February 23, 1990. The U.S. patent was issued as U.S. Patent No. 4,995,082, on February 19, 1991.

3. Claim 5 of my patent describes a general method for preprocessing signatures that are based on a discrete logarithm.

After my patent was issued, Peter de Rooij found weaknesses in two specific instances of the general method described in Claim 5. These specific weaknesses do not apply to the general method described in the patent. However, the general method must be applied with some care to preserve the security of the digital signatures.

4. After de Rooij published his work, my students and I further developed the general method described in Claim 5. We have examples of the general method which are efficent and provably secure. Some of these methods are described in the master's thesis of my student Johannes Merkle, "On Schnorr's Preprocessing Method," which was published in 1994.

5. The other features of my invention are independent of the preprocessing method described in Claim 5. In particular, the digital signature generation method described in Claim 6 can well be used without the particular preprocessing method of Claim 5. Therefore, the validity of the other claims is not related to the utility of Claim 5.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on November 14, 1995 at Frankfurt, Germany.

C.P. Schnorr

Claus P. Schnorr